

## UNITED STATES DISTRICT COURT

for the

Northern District of New York

U.S. DISTRICT COURT - N.D. OF N.Y.

FILED

Apr 10 - 2023

John M. Domurad, Clerk

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)The Locations and Items as further described in  
Attachment A

Case No. 3:23-MJ- 209 (ATB)

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The Locations and Items as further described in Attachment A

located in the Northern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
Title 18, United States Code, Section 2422(b)	Attempted Enticement of a Minor

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jenelle Corrine Bringuel, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
Telephone (specify reliable electronic means).

Date: 04/10/2023City and state: Syracuse, New York

Judge's signature

Hon. Andrew T. Baxter, U.S. Magistrate Court Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANTS**

JENELLE CORRINE BRINGUEL, being duly sworn, deposes and states:

**INTRODUCTION**

1. I am a Special Agent of the United States Department of Justice, Federal Bureau of Investigation (“FBI”), and I am empowered by law to investigate and make arrests for offenses enumerated in Title 18, United States Code, Section 2516. As such, I am an “investigative or law enforcement officer” within the meaning of Title 18, United States Code, Section 2510(7).

2. I have been employed as a Special Agent of the FBI since June 2012 and am currently assigned to the Albany Division, Binghamton Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to cybercrime, child exploitation, and child pornography. I have gained experience through training by the FBI and everyday work relating to conducting these types of investigations. I have participated in the execution of several federal search warrants in child sexual exploitation investigations.

3. I make this affidavit in support of an application under Rule 4.1 of the Federal Rules of Criminal Procedure for warrants to search the following:

(A) A 2016 Dodge Ram pickup truck, grey in color, New York license plate JMT-1878, registered to Joel Cook (the “**SUBJECT VEHICLE**”)

(B) Any computers, cellular telephones, tablets, computer equipment, computer storage media and electronic storage media found in the vehicle (the “**DEVICES**”).

for evidence, fruits, and instrumentalities relating to violations of Title 18, United States Code, Section 2422(b) (attempted enticement of a minor), as more fully described in Attachment B.

4. The facts in this affidavit come from my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

**PROBABLE CAUSE**

5. On March 13, 2023, the grandmother of a 14-year-old female child (V1) contacted the Tompkins County Sheriff's Office to report that Joel Cook, a 48 year old man who is known to her family, had been sending inappropriate sexual text messages and photographs to her granddaughter. V1's mother and grandmother provided law enforcement with access to V1's phone, where text messages between V1 and Cook were observed.

6. Through the family's relationship with Cook, V1 has had occasion to visit and spend the night at Cook's home.

7. Following the disclosure by her grandmother and a review of the text messages on her phone, V1 was interviewed by a child forensic interviewer. In the interview, V1 disclosed that, on numerous occasions beginning in or about January 2023, while staying at Cook's house, Cook approached V1 while others were sleeping and touched her breasts, buttocks, and vaginal area over her clothing, and that he also rubbed her sides and kissed her neck. V1 stated that, more than once, Cook attempted to get her to touch his penis, but she pulled away. She disclosed that Cook told V1, "This stays between you and me."

8. On March 12, 2023, the defendant sent the following text message to V1:

COOK: I have your number saved now and remember everything stays  
between you and me

V1 did not respond to this message.

9. On March 13, 2023, the defendant sent the following text messages to V1:

COOK: For us only  
And this is the start of your wanting to learn  
  
Everything else is fine with me and you know that you have the say  
for everything you want

COOK: [sends two images]:  
The first image contains a banner from “Porn hub” and the title “My  
Perv Family  
  
The second image depicts a woman with an erect penis in her mouth.

COOK: I can not wait to talk with you more

Again, V1 did not respond.

10. On March 16, 2023, the defendant sent the following text message to V1:

COOK: Hi sweetie wear your nice leggings and undies this weekend and  
DELETE ALL TEXT FROM ME AND REMEMBER THAT IT IS  
BETWEEN YOU AND ME ONLY

V1 did not respond.

11. After the above text messages were sent to V1, the child’s phone was turned over to law enforcement, and agents thereafter assumed V1’s identity in text messages with COOK. From March 17, 2023, until April 7, 2023, law enforcement continued to exchange photo and text messages with COOK posing as V1. These messages were indicative of COOK’s desire and intention to have sexual contact with V1.

12. From April 4-5, 2023, COOK made arrangements with law enforcement posing as V1 to meet on April 8, 2023. COOK agreed to pick V1 up at a residence in Tompkins County, New York.

13. On April 8, 2023, COOK arrived at the Tompkins County, New York location where he had made arrangements to meet V1. Following his arrest, COOK admitted in a

Mirandized recorded interview that he was the individual who had been communicating with V1 via text messages. COOK was confronted with the text message conversations between he and V1, of which portions were read to him. COOK admitted engaging in the text message conversations and that the picture sent to V1 of an adult male penis was his. COOK admitted he engaged in conversations with V1 to ensure she knew he could trust him like a father figure and feel comfortable discussing anything with him, including sex.

14. COOK drove the **SUBJECT VEHICLE** to the meet with V1 on April 8, 2023. During the interview, COOK stated that he left his cell phone back at his residence due to the fact the battery was almost dead. COOK stated he only uses one cell phone; however, there is a second cell phone on his plan that belongs to his son. COOK stated that his son does not use his (COOK's) cell phone nor does COOK use his son's phone.

15. Law enforcement drove the **SUBJECT VEHICLE** from the scene to the New York State Police barracks in Freeville, NY. A cell phone was observed in plain view by law enforcement in the front middle portion of the vehicle between the driver and passenger seats.

14. The acts the defendant discussed engaging in with V1 would violate the following statutes, among others: (1) Criminal Sexual Act in the Second Degree, New York Penal Law, Section 130.45(1) which makes it unlawful for a person eighteen years old or more to engage in oral sexual conduct with another person less than fifteen years old, and (2) Sexual Abuse in the Third Degree, New York Penal Law, Section 130.55 which makes it unlawful to subject another person to sexual contact without the latter's consent. Under New York Law, Section 130.05(3)(a) a person is deemed incapable of consent when he or she is less than seventeen years old.

**COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

15. As described above and in Attachment B, this application seeks permission to search for records, in whatever form they are found, including data stored on a computer, hard drive or other electronic/digital storage media. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

16. *Probable cause.* I submit that if a computer or storage medium is found during the course of the execution of the search warrants, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
- e. Based upon my training and experience and conversations with other law enforcement personnel, I am aware that a number of computer storage devices are quite small and portable, and can be easily hidden on a person or easily concealed in other locations. For instance, digital cameras can store numerous digital images on a disk approximately the size of a postage stamp. In addition, thumb drives, which are approximately the size of a pocket knife, can hold numerous images and computer videos.

17. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any seized storage medium because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and

malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log computer user account session times and durations, computer activity associated with user accounts, electronic storage media that is or was connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or

consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrants.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user’s intent.
- f. I know that when an individual uses a computer to possess, receive, or distribute child pornography, the individual’s computer or device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for

evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

18. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrants. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrants call for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of

information. Reviewing that information for things described in the warrants can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under these warrants could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

### **BIOMETRIC ACCESS TO DEVICES**

19. The requested warrants would also permit law enforcement to compel Joel Cook to unlock any devices requiring biometric access subject to seizure pursuant to these warrants. The grounds for this request are as follows:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint

scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.
- d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft

devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

- e. In my training and experience, users of electronic devices often enable these biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- f. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the **DEVICES** subject to search under these warrants currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by these warrants.
- g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such

features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

20. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to these warrants and may be unlocked using one of these biometric features, the requested warrants would permit law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Joel Cook to the fingerprint scanner of the devices; (2) hold the devices in front of Joel Cook's face and activate the facial recognition feature; and/or (3) hold the devices in front of Joel Cook's face and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by these warrants. The proposed warrants do not authorize law enforcement to require that Joel Cook state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrants do not authorize law enforcement to require Joel Cook to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

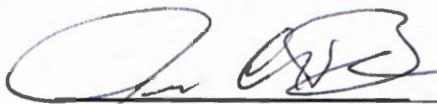
**LAW ENFORCEMENT AGENCIES ASSISTING FBI**

21. These search warrants will be executed by your Affiant and other FBI Special Agents, however, law enforcement officers from other agencies, including the New York State Police (NYSP), may be utilized by the FBI in the execution of these search warrants, to include the forensic examination of any electronic storage media devices that may be seized and later analyzed at either an FBI or NYSP computer forensic laboratory.

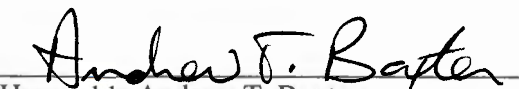
**CONCLUSION**

22. As stated above, there is probable cause to believe that evidence of criminal offenses, namely, violations of Title 18, United States Code, Section 2422(b) (attempted enticement of a minor) exist and are concealed at, on, or within the locations and items to be searched as outlined in Attachment A.

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH THE REQUIREMENTS OF RULE 4.1 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE.

  
Jenelle Corrine Bringuel  
Special Agent  
Federal Bureau of Investigation

I, the Honorable Andrew T. Baxter, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on April 10 2023, in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.

  
Honorable Andrew T. Baxter  
United States Magistrate Judge  
Northern District of New York

**ATTACHMENT A**  
**LOCATIONS AND ITEMS TO BE SEARCHED**

The locations and items to be searched are:

(A) 2016 Dodge Ram pickup truck, grey in color, New York license plate JMT-1878, registered to Joel Cook (the “**SUBJECT VEHICLE**”)

(B) Any computers, cellular telephones, tablets, computer equipment, computer storage media and electronic storage media found in the **SUBJECT VEHICLE** (the “**DEVICES**”).

**ATTACHMENT B**  
**LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED**

Items of evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, namely, violations of 18 U.S.C. § 2422(b) (attempted enticement of a minor):

**Computers and Electronic Media**

1. The authorization includes the search of electronic data to include deleted data, remnant data, and slack space. The seizure and search of the **DEVICES** will be conducted in accordance with the affidavit submitted in support of this warrant.
2. Computer hardware, meaning any and all computer equipment, including any electronic storing devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as thumb drives, flash drives, sd (secure digital) cards, fixed disks, external and internal hard drives and disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing, or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).
3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems, software, application software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.
4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
5. Computer passwords and data security devices, meaning any devices, programs, or data, whether themselves in the nature of hardware or software, that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and

similar information that is required to access computer programs or data, or to otherwise render programs or data into usable form.

6. Any computer or electronic records, documents and materials referencing or relating to the above-described offense. Such records, documents or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing or typing); any electrical, electronic or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as thumb drives, flash drives, sd (secure digital) cards, floppy diskettes, hard disks, CD-ROMs, DVDs, optical disks, printer buffers, soft cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form that such information might take includes, but is not limited to, thumb drives, flash drives, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, DVDs, video cassettes, and other media capable of storing magnetic or optical coding.

8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data, obtained through computer or Internet-based communications, including data in the form of electronic records, documents and materials, including those used to facilitate interstate communications, included but not limited to telephone (including mobile telephone) and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding, on computer media, or on media capable of being read by a computer or computer-related equipment, such as thumb drives, flash drives, sd (secure digital) cards, fixed disks, external hard disks, removable hard disk cartridges, CDs, DVDs, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

### **Computer and Internet Records**

9. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes (however and wherever written, stored or maintained), books, notes, and reference materials.

10. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.

11. Records of address or identifying information for the target of the investigation and any personal or business contacts or associates of his, (however and wherever written, stored or

maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., “Nics”), user ID’s, eID’s (electronic ID numbers) and passwords.

12. Documents and records, in any form or format, regarding the identity of any person using the identity of registered user 607-342-8046, a phone number known to be associated with COOK.

13. Documents and records regarding the ownership and/or possession of the searched premises.

14. Computer records and evidence identifying who the particular user was who received, downloaded, possessed, or accessed with intent to view any child pornography found on any computer or computer media (evidence of attribution), or who attempted to do any of the foregoing, and how the computer was used to effectuate that activity.

### **Materials Relating to Child Erotica and Depictions of Minors**

15. Any and all visual depictions of minors, including, but not limited to, sexually explicit images of minors.

16. Any and all chats, chat logs, emails, and other text documents, describing or relating to sexually explicit conduct with children, as well as fantasy writings regarding, describing, or showing a sexual interest in children.

17. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18 United States Code, Section 2256(2).

18. Any and all notebooks and any other records reflecting personal contact, and any other activities, with minors who may be visually depicted while engaged in sexually explicit conduct, or engaged in sexually explicit chat, email, or other communications.

19. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, notes, and sexual aids.

20. Evidence of chat communications with the law enforcement officers posing as V1, to include images that were exchanged.

### **Biometric Unlocking**

During the execution of the search warrant, law enforcement personnel are also authorized to compel Joel Cook to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of any of the **DEVICES** found during the course of the execution of this warrant.

This warrant does not authorize law enforcement personnel to request that Joel COOK state or otherwise provide the password or any other means that may be used to unlock or access the

**DEVICES**, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the **DEVICES**.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.